AlliedWare^{TM} OS

How To | Configure VPNs in a Corporate Network, with Optional Prioritisation of VoIP

Introduction

In this How To Note's example, a headquarters office has VPNs to two branch offices and a number of roaming VPN clients. The example illustrates the following possible components that you could use in a corporate network:

- VPNs between a headquarters office and roaming VPN clients, such as travellers' laptops
- VPNs between a branch office and roaming VPN clients, such as travellers' laptops
- a VPN between a headquarters office and a branch office with a fixed IP address, when the branch office has an ADSL PPPoA connection to the internet
- a VPN between a headquarters office and a branch office with a dynamically assigned IP address, when the branch office has an ADSL PPPoEoA connection to the internet
- using software QoS to prioritise voice (VoIP) traffic over the VPNs

Select the solution components that are relevant for your network requirements and internet connection type.

Contents

Which products and software versions does this information apply to?

The information provided in this document applies to the following products:

- AR400 Series routers
- AR750S and AR770S routers
- Rapier and Rapier i Series switches
- AT-8800 Series switches

running software version 2.6.6 and above. However, prioritising the voice traffic requires Software Quality of Service, which is available with version 2.7.1 and above.

On the roaming VPN clients, we tested this solution with Microsoft® Windows Virtual Private Network.

This How To Note shows how to prioritise VoIP traffic at the offices, but does not show how to set up the VoIP facility itself on your VPN client PCs. You need to find suitable PC software to provide that.

Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

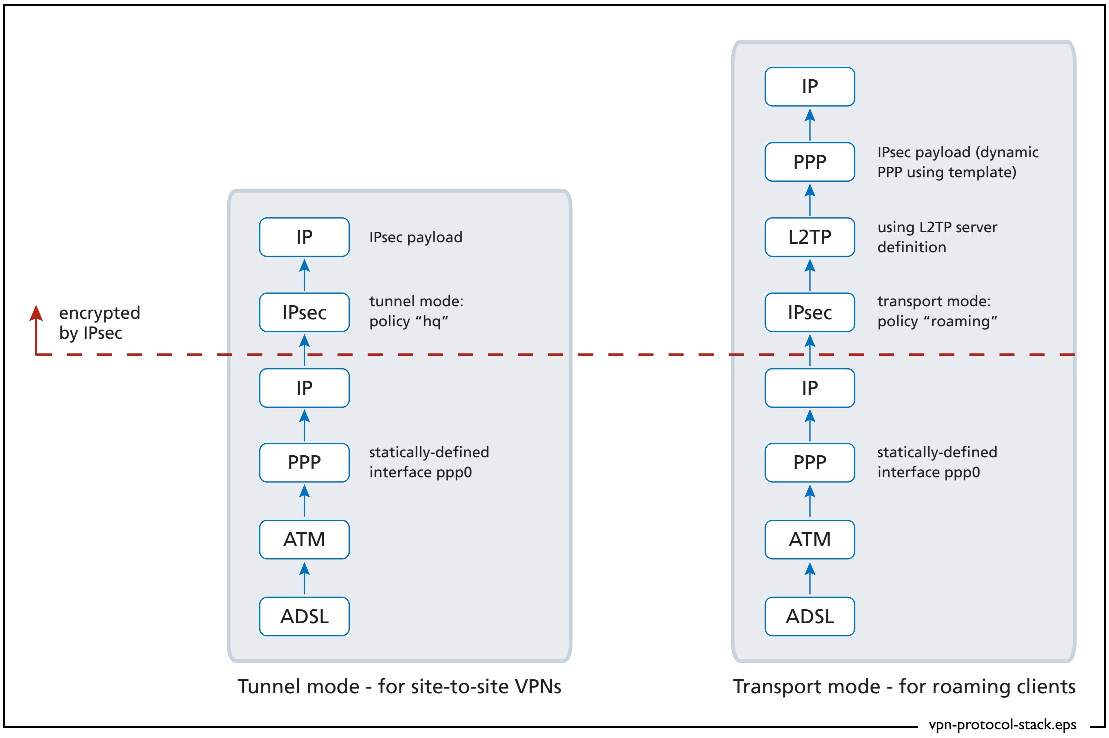
For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

About IPsec modes: tunnel and transport

This solution uses two types of VPN:

- IPsec tunnel mode, for the headquarters office to branch office VPNs. These are site-to-site (router-to-router) VPNs.
- IPsec transport mode with L2TP, for the roaming Windows VPN clients.

The following figure shows the protocol stacks for the tunnel mode VPN and the transport mode VPN for the connection type PPPoA.



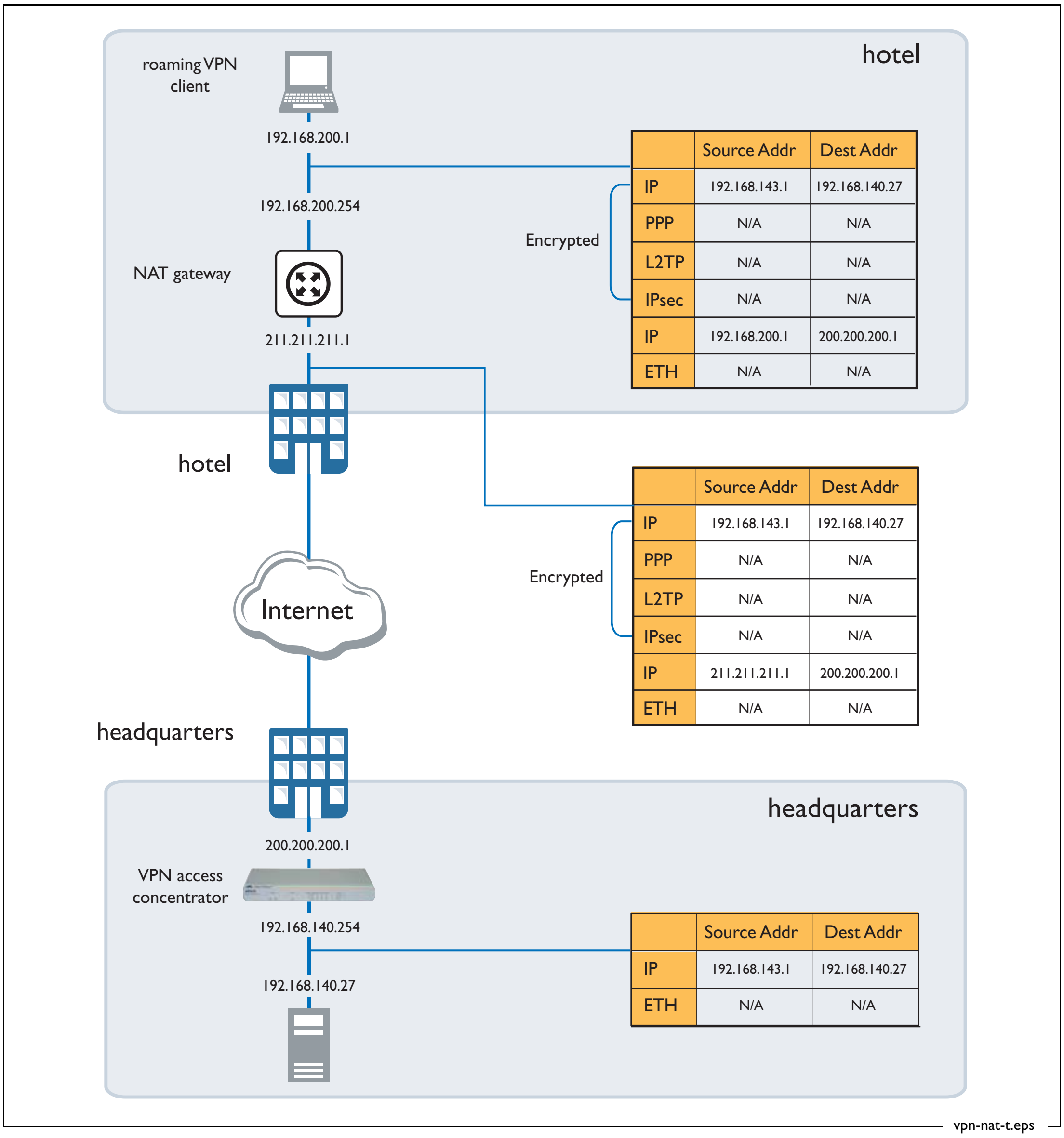
In this How To Note, branch office 1 uses PPPoA. The other offices in this How To Note use different connection types and therefore have different stacks below IP. Branch office 2 uses PPP over virtual Ethernet over ATM, and headquarters simply uses IP over an actual Ethernet WAN connection.

Background: NAT-T and policies

NAT-T NAT Traversal (NAT-T) can be enabled on any of our IPsec VPN links. It automatically allows IPsec VPNs to traverse any NAT gateways that may be in the VPN path. This is likely to occur with the VPNs from the roaming VPN clients—they are likely to use a LAN at a remote site that is behind a NAT gateway.

NAT-T may also be applicable for a site-to-site VPN, if one of the routers is behind a NAT gateway, such as some ADSL devices. Note that AR44xS series routers provide an ADSL interface, which removes the need for a separate ADSL device. Therefore, the examples in this How To Note do not include NAT-T for the site-to-site VPNs.

The following figure shows how the addresses in the IPsec headers change as a packet from a roaming client traverses NAT gateways in the VPN pathway. The figure illustrates IPsec transport mode with L2TP.



	Source Addr	Dest Addr
IP	192.168.143.1	192.168.140.27
PPP	N/A	N/A
L2TP	N/A	N/A
IPsec	N/A	N/A
IP	192.168.200.1	200.200.200.1
ETH	N/A	N/A

	Source Addr	Dest Addr
IP	192.168.143.1	192.168.140.27
PPP	N/A	N/A
L2TP	N/A	N/A
IPsec	N/A	N/A
IP	211.211.211.1	200.200.200.1
ETH	N/A	N/A

	Source Addr	Dest Addr
IP	192.168.143.1	192.168.140.27
ETH	N/A	N/A

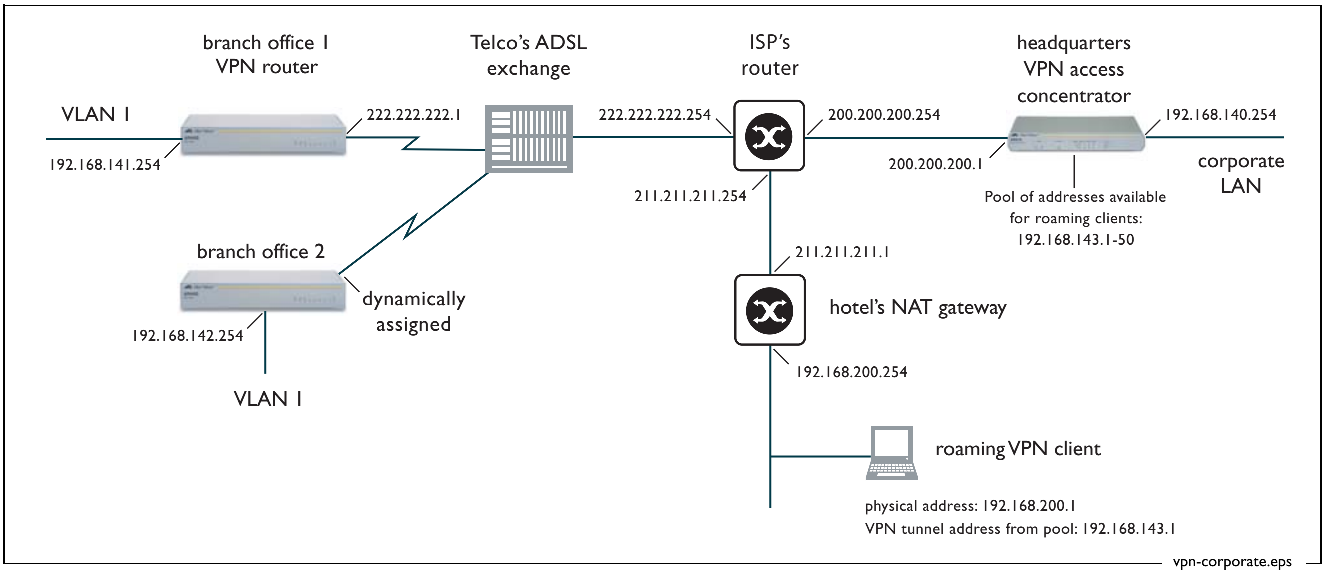
Policies and interfaces

It is useful to keep in mind that you apply firewall rules and IPsec policies to interfaces in the following different ways:

- Firewall rules can be applied on either private or public interfaces. The rules are matched against traffic that comes into the interface to which they were applied. Rules applied to private interfaces are typically quite different to rules applied to public interfaces.
- IPsec policies are applied only on the public interface. The policy definitions, and any active Security Associations (SAs), are considered for both incoming and outgoing traffic on that interface.

How to configure VPNs in typical corporate networks

This section describes a typical corporate network using secure VPN. The network consists of a headquarters (HQ) router and two branch office routers. The headquarters router is acting as a VPN Access Concentrator, and allows for VPN access from either of the branch office sites or from roaming laptop VPN clients. The network is illustrated in the following figure.



Branch office 1 uses the PPPoA ADSL link type, and branch office 2 uses the PPPoEoA ADSL link type. We have done this to illustrate these two commonly used ADSL link types. For information about the ADSL link type you need, see your ADSL provider.

This How To Note gives you the commands for configuring each of the following:

1. The headquarters VPN access concentrator router, which includes:
   - an ethernet connection to the Internet
   - a fixed Internet address. This means that the branch offices and the roaming VPN clients have a known target for the headquarters end of the VPN
   - VPN access to and from branch office 1. This can be initiated from the headquarters or branch office end. This is a site-to-site VPN and uses IPsec tunnel mode (see "Background: NAT-T and policies" on page 4).
   - VPN access from branch office 2. This can only be initiated from the branch office end, because the branch office has a dynamically-assigned IP address. This also uses IPsec tunnel mode.
   - VPN client access from roaming users on Windows 2000 and Windows XP. This is provided by using IPsec transport mode with L2TP (see "About IPsec modes: tunnel and transport" on page 3)
   - optionally, prioritisation of voice (VoIP) traffic for these VPN clients by using Software Quality of Service (SQoS). If the VPN clients use VoIP to establish voice calls via the headquarters network, this helps maintain voice quality.

2. The branch office 1 router, which provides:
    - an ADSL PPPoA Internet connection. Note that the PPPoA connection requires an ATM DSLAM
    - VPN access to headquarters using IPsec tunnel mode
    - incoming VPN client access from roaming users
    - a fixed Internet address so that roaming VPN clients have a known target for the branch office end of the VPN
3. The branch office 2 router, which provides:
    - an ADSL PPPoEoA Internet connection
    - VPN access to headquarters using IPsec tunnel mode
    - a dynamically assigned Internet address, as used by many ISPs.

Color coding For your convenience, the configurations are color-coded:

🟩 headquarters 🟫 branch office 1 🟦 branch office 2

Before you start

Don’t forget to check you have the following when planning your secure VPN network:

1. ISAKMP shared key
2. Fixed public IP addresses to use where appropriate
3. The IP subnets to use on private LANs at the branch and headquarters sites
4. The range of IP addresses to use in the IP pools for allocating to the remote users
5. Usernames and passwords for the remote users
6. IP addresses from which SSH connections can be made to the routers (if applicable)
7. Connection parameters for the ADSL connections at the branch offices
8. VPN client PCs set up, as described in the How To Notes in "Related How To Notes" on page 2.

How to configure the headquarters VPN access concentrator

Before you begin to configure your router, ensure that it is running the appropriate software release, patch and GUI files and has no configuration.

```
set inst=pref rel=<rel-file> pat=<patch-file> gui=<gui-file>

set conf=none

disable system security

restart reboot
```

Note: A software QoS extension to this configuration, to prioritise VoIP traffic over the VPNs, is available in "How to prioritise outgoing VoIP traffic from the headquarters router" on page 31.

1. Configure general system and user settings

Name the router

```
set system name=HQ
```

Define a security officer.

```
add user=secoff pass=<your-secoff-password> priv=securityofficer
   lo=yes telnet=yes
```

Do not forget your "secoff" password.

Enable security mode so that VPN keys are stored securely, and other security features are enabled.

```
enable system security
```

Once security mode is enabled, you need to log in as a security officer to enter most configuration-altering commands.

```
login secoff

password: <your-secoff-password>
```

It is important to keep this security officer username and password secure, and to consider proper handover of it in the event of IT staff changes.

Also, we recommend you leave a "manager" privilege user defined because this may provide backup access if the security officer password is lost. Do not leave the manager password at the factory default—change it to a password in keeping with your company's security policy.

```
set user=manager password=<your-company-policy-password>
```

When security mode is enabled, router configuration access times out after inactivity to prevent unauthorised access. The default timeout is 60 seconds, but you may temporarily raise it to 600 seconds if desired.

```
set user securedelay=600
```

2. Configure IP for internet access

Give a fixed public address to the interface eth0, which is the Internet connection interface. You can replace eth0 with ppp0 if you use a leased line.

```
enable ip

add ip int=eth0 ip=200.200.200.1
```

Give a fixed private address to the interface vlan1, which connects the router to the headquarters LAN.

```
add ip int=vlan1 ip=192.168.140.254
```

Set the default route. The next hop is the gateway address provided by the ISP.

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.200.200.254
```

If desired, set up the router as a DHCP server for the headquarters LAN.

```
create dhcp policy=hq lease=7200

add dhcp policy=hq rou=192.168.140.254

add dhcp policy=hq subn=255.255.255.0

create dhcp range=hq_hosts policy=hq ip=192.168.140.16 num=32

ena dhcp
```

3. Configure remote management access, if desired

If you need remote management access, we strongly recommend that you use Secure Shell (SSH). You should not telnet to a secure gateway.

To configure SSH, define appropriate RSA encryption keys, then enable the SSH server.

```
create enco key=2 type=rsa length=1024 description="host key"
   format=ssh

create enco key=3 type=rsa length=768 description="server key"
   format=ssh

enable ssh server serverkey=3 hostkey=2
```

Enable the user who connects via SSH to log in as secoff, by adding the secoff user as an SSH user. Also, you may choose to restrict access so that it is only permitted from particular addresses.

```
add ssh user=secoff password=<secoff-password>
   ipaddress=<trusted-remote-ip-address>
   mask=<subnet-mask-of-trusted-hosts>

disable telnet server
```

Secure Shell is a more secure, encrypted method of remote management access than telnet. If you need to use telnet, even though it is insecure, you should restrict access by defining remote security officers (RSOs). RSO definitions specify trusted remote addresses for security officer users.

```
add user rso ip=<ipadd>[-<ipadd>]

enable user rso

enable telnet server
```

4. Capture status information remotely, if desired

If desired, set the router to send log messages to a syslog server.

```
create log output=2 destination=syslog server=<syslog-server-address>
    syslogformat=extended

add log out=2 filter=1 sev=>3
```

If desired, you can configure SNMP to inform you or your service provider of network events, such as the LAN interface of the router going down. We recommend SNMPv3 for security reasons. For details, see *How To Configure SNMPv3 On Allied Telesis Routers and Managed Layer 3 Switches*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

5. Configure dynamic PPP over L2TP connections

You need to configure dynamic PPP over L2TP to accept incoming Windows VPN client connections.

Create an IP pool to allocate unique internal payload addresses to incoming VPN clients.

```
create ip pool=roaming ip=192.168.143.1-192.168.143.50
```

Define a PPP template. This defines authentication and uses the IP pool of addresses.

```
create ppp template=1

set ppp template=1 bap=off ippool=roaming authentication=chap echo=10
    lqr=off
```

Configure L2TP. When the router successfully negotiates an L2TP tunnel connection from any remote peer, it then creates a PPP interface over that tunnel, using the PPP parameters defined by the PPP template. If you intend to prioritise voice traffic (see page 30), also turn on TOS (type of service) reflection, so that DSCP marked VoIP packets can be classified for prioritisation at the PPP level.

```
enable l2tp

enable l2tp server=both

add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1 tos=on
```

Add your approved roaming VPN client usernames.

```
add user=roaming1 pass=roaming1 lo=no telnet=no

add user=roaming2 pass=roaming2 lo=no telnet=no
```

If desired, you can instead use a RADIUS authentication server.

```
add radius server=<radius-server-address> secret=<secret-key>
```

6. Check feature licences

Check that you have a 3DES feature licence for the ISAKMP policies.

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor.

If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

7. Configure the VPNs for the branch offices and roaming clients

Enable IPsec

```
enable ipsec
```

In this example, IPsec SA specifications propose:

- ISAKMP as the key management protocol
- ESP as the IPsec protocol
- (for site-to-site VPNs) 3DESOUTER as the encryption algorithm for ESP
- (for site-to-site VPNs) SHA as the hashing algorithm for ESP authentication
- (for roaming client VPNs) four possible variants of VPN encryption, for added flexibility. We propose the most secure option first.

Create an SA specification for the branch office site-to-site VPN. This SA specification uses tunnel mode by default.

```
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
```

Create a group of SA specifications for the roaming VPN clients. These SA specifications use IPsec transport mode for Windows VPN interoperability. Multiple specifications allow IPsec to negotiate different levels of encryption to match what your version of the VPN client provides.

```
create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=sha
   mod=transport

create ipsec sas=3 key=isakmp prot=esp enc=3desouter hasha=md5
   mod=transport

create ipsec sas=4 key=isakmp prot=esp enc=des hasha=sha mod=transport

create ipsec sas=5 key=isakmp prot=esp enc=des hasha=md5 mod=transport
```

Create two IPsec bundles, one for the remote branch routers and one for the roaming VPN clients.

```
create ipsec bund=1 key=isakmp string="1"

create ipsec bund=2 key=isakmp string="2 or 3 or 4 or 5"
```

Create IPsec policies to bypass IPsec for ISAKMP messages and the “port floated” key exchange that NAT-T uses.

```
create ipsec pol=isakmp int=eth0 ac=permit lp=500 rp=500

create ipsec pol=isakmp_float int=eth0 ac=permit lp=4500
```

Create an IPsec policy for the VPN traffic between headquarters and branch office 1. Identify the traffic by its local and remote addresses—in this example the subnet used on the LAN at branch office 1 (remote) is 192.168.141.0/24. Note that the local address selector is wider than the headquarter’s LAN; in fact, we cover all site subnets with this supernet.

```
create ipsec pol=branch1 int=eth0 ac=ipsec key=isakmp isa=branch1
   bund=1 peer=222.222.222.1 lad=192.168.0.0 lma=255.255.0.0
   rad=192.168.141.0 rma=255.255.255.0
```

Create another IPsec policy for the VPN traffic between headquarters and branch office 2. The subnet used on the LAN at branch office 2 is 192.168.142.0/24. This policy uses **peeraddress=dynamic**. The **dynamic** option is designed for only one dynamic peer to connect at a time under that policy, which makes sense when the policy is intended for one branch office.

```
create ipsec pol=branch2 int=eth0 ac=ipsec key=isakmp isa=branch2
   bund=1 peer=dynamic lad=192.168.0.0 lma=255.255.0.0
   rad=192.168.142.0 rma=255.255.255.0
```

Create another IPsec policy for roaming VPN clients to access headquarters. Identify the traffic by the L2TP port (UDP traffic to port 1701). This policy uses **peeraddress=any**. The **any** option allows simultaneous VPN clients to be set up under the policy.

```
create ipsec pol=roaming int=eth0 ac=ipsec key=isakmp bund=2 peer=any
   isa=roaming lp=1701 tra=udp
```

Create another IPsec policy for direct Internet traffic from the headquarters LAN to the Internet, such as web browsing.

```
create ipsec pol=internet int=eth0 ac=permit
```

Note: The order of the IPsec policies is important. The Internet permit policy must be last.

Create your ISAKMP pre-shared key. This key is used when initiating your VPN during phase one ISAKMP exchanges with your VPN peers. Share the value of this pre-shared key with all VPN peers that use it—in this example, the roaming VPN clients and the branch office routers. The router only uses this key during phase one ISAKMP exchanges.

```
create enco key=1 type=general value=<alphanumeric-preshared-key>
```

Enable ISAKMP.

```
ena isa
```

This example uses separate ISAKMP policies for each peer. Note the following points about the policies:

- different ISAKMP policies meet the different needs of the different types of peer—Allied Telesis routers *versus* Windows VPN clients. For example, Allied Telesis peers support heartbeats; Windows VPN clients do not.

- the branch office policies use a different encryption transform—3des2key—than the roaming policy. When a new incoming ISAKMP message starts, this lets the router identify whether to match it to the roaming policy or one of the branch office policies.
- the policies include local IDs. These allow the remote peers to identify incoming ISAKMP packets from the headquarters router through any NAT gateways in the path.

Create an ISAKMP policy for the VPN to branch 1, with a fixed address. Use ISAKMP heartbeats, which allow ISAKMP to clear SAs if either end of the link resets.

```
create isakmp pol=branch1 pe=222.222.222.1 sendd=true key=1 heart=both
    encalg=3des2key localid=hq
```

Create an ISAKMP policy for the VPN to branch 2, with **peer=any** because the branch 2 router has a dynamic address.

```
create isakmp pol=branch2 pe=any sendd=true key=1 heart=both
    encalg=3des2key localid=hq
```

Create an ISAKMP policy for VPNs to roaming VPN clients, with **peer=any** because the peers have dynamic addresses. Note that you cannot use heartbeats with Windows peers. We recommend that you enable NAT-T, because the roaming VPN clients will sometimes need to connect through a NAT-T gateway.

```
create isakmp pol=roaming pe=any key=1 sendd=true natt=true sendi=on
    localid=hq2
```

The roaming policy uses the same key as the branch office policies. If you want to, you can instead generate a unique pre-shared key to use with the roaming clients, and attach it to the roaming policy.

8. Configure the firewall's basic settings

Enable the firewall and create a firewall policy.

```
enable firewall

create firewall policy=hq

enable firewall policy=hq icmp_f=all
```

Specify the LAN-facing interface of the router as a private (trusted) interface on the firewall.

```
add firewall policy=hq int=vlan1 type=private
```

Specify the Internet-facing interface of the router as a public (not trusted) interface on the firewall.

```
add firewall policy=hq int=eth0 type=public
```

Define a firewall dynamic definition to enable dynamically created interfaces to participate in the firewall. In this case, the definition provides for the dynamic PPP over L2TP interfaces that incoming Windows VPN connections use. In other words, when the router dynamically creates PPP interfaces over the L2TP connections from the roaming PC clients, the router automatically adds these dynamic interfaces as private interfaces on the firewall. The router can trust traffic arriving on the dynamic interfaces because—in this example configuration—it can only come from an authenticated and encrypted VPN connection.

```
create firewall policy=hq dynamic=roaming

add firewall policy=hq dynamic=roaming user=any

add firewall policy=hq int=dyn-roaming type=private
```

Define NAT definitions to use when traffic from the local LAN accesses the Internet and to allow Internet access for remote VPN client users.

```
add firewall policy=hq nat=enhanced int=vlan1 gblin=eth0

add firewall policy=hq nat=enhanced int=dyn-roaming gblin=eth0
```

Note: Windows VPN client default behaviour does not support "split tunnelling". This means that when the Windows VPN tunnel is up, all traffic passes through it, whether the traffic is destined for the headquarters office LAN or for Internet surfing destinations. Therefore, we suggest you define the second NAT above, to allow clients to access the Internet via the headquarters router when their VPN connection is up.

9. Configure the firewall's access rules

Create a rule to allow incoming ISAKMP negotiation messages to pass through the firewall.

```
add firewall policy=hq ru=1 ac=allo int=eth0 prot=udp po=500
    ip=200.200.200.1 gblip=200.200.200.1 gblp=500
```

Create a rule to support NAT-T. If a NAT gateway is detected in the VPN path, NAT-T "port floats" IKE to port 4500, and also encapsulates IPsec inside UDP headers to the same port. Therefore, UDP traffic to port 4500 must be allowed to pass through the firewall.

```
add firewall policy=hq ru=2 ac=allo int=eth0 prot=udp po=4500
    ip=200.200.200.1 gblip=200.200.200.1 gblp=4500
```

Create a rule for the roaming VPN clients. Windows VPN client uses L2TP (UDP to port 1701) encapsulated inside IPsec. This rule allows L2TP traffic through the firewall if it originally arrived at the router encapsulated in IPsec (and was decapsulated by the IPsec process before it passed to the firewall).

```
add firewall policy=hq ru=3 ac=allo int=eth0 prot=udp po=1701
    ip=200.200.200.1 gblip=200.200.200.1 gblp=1701 enc=ips
```

Create a pair of rules to allow office-to-office payload traffic to pass through the firewall without applying NAT. This traffic must bypass NAT so that the traffic matches subsequent IPsec policy address selectors. You need two rules—one for the public interface and one for the private interface—so that office-to-office payload traffic bypasses NAT regardless of which side initiated the session.

The rule for the public interface uses **encapsulation=ipsec** to identify incoming VPN traffic—decrypted payload data that came from the IPsec module.

```
add firewall policy=hq ru=4 ac=non int=eth0 prot=all enc=ips
```

The rule for the private interface uses both source and destination addresses to identify outgoing VPN traffic.

```
add firewall policy=hq ru=5 ac=non int=vlan1 prot=all
   ip=192.168.140.1-192.168.140.254 rem=192.168.141.0-192.168.144.254
```

If you configured SSH (recommended), create a rule to allow SSH traffic to pass through the firewall.

```
add firewall policy=hq ru=6 ac=allo int=eth0 prot=tcp po=22
   ip=200.200.200.1 gblip=200.200.200.1 gblp=22
```

If you instead stayed with telnet (not recommended) and configured RSOs, create a rule to allow telnet traffic to pass through the firewall.

```
add firewall policy=hq ru=7 ac=allo int=eth0 prot=tcp po=23
   ip=200.200.200.1 gblip=200.200.200.1 gblp=23
```

10. Save your configuration

It is important to save your configuration when you finish, to preserve the configuration over any power cuts.

```
create conf=<your-file.cfg>
```

This is particularly important in security configurations because it preserves the security officer definition. Without this, regaining configuration access would destroy encryption information such as keys.

Once you have saved the configuration to a file, specify that file as the configuration script to use when the router boots up.

```
set config=<your-file.cfg>
```

Note: If you forget your secoff user password, log in as manager. The manager user cannot edit a router in system security mode, so enter the command **disable system security**. This destroys your encryption keys. Edit your configuration file to redefine your secoff user password, then reboot, then log in as secoff, then enable system security again, then recreate the keys.

How to configure the AR440S router at branch office 1

Before you begin to configure your router, ensure that it is running the appropriate software release, patch and GUI files and has no configuration.

```
set inst=pref rel=<rel-file> pat=<patch-file> gui=<gui-file>

set conf=none

disable system security

restart reboot
```

Note: A software QoS extension to this configuration, to prioritise VoIP traffic over the VPNs, is available in "How to prioritise outgoing VoIP traffic from the branch office 1 router" on page 33.

1. Configure general system and user settings

Name the router

```
set system name=Branch1
```

Define a security officer.

```
add user=secoff pass=<your-secoff-password> priv=securityofficer
   lo=yes telnet=yes
```

Do not forget your “secoff” password.

Enable security mode so that VPN keys are stored securely, and other security features are enabled.

```
enable system security
```

Once security mode is enabled, you need to log in as a security officer to enter most configuration-altering commands.

```
login secoff

password: <your-secoff-password>
```

It is important to keep this security officer username and password secure, and to consider proper handover of it in the event of IT staff changes.

Also, we recommend you leave a “manager” privilege user defined because this may provide backup access if the security officer password is lost. Do not leave the manager password at the factory default—change it to a password in keeping with your company's security policy.

```
set user=manager password=<your-company-policy-password>
```

When security mode is enabled, router configuration access times out after inactivity to prevent unauthorised access. The default timeout is 60 seconds, but you may temporarily raise it to 600 seconds if desired.

```
set user securedelay=600
```

2. Configure ADSL for internet access

Create your Asymmetric Digital Subscriber Line (ADSL) connection. Asynchronous Transfer Mode (ATM) is always used over ADSL.

```
enable adsl=0

create atm=0 over=adsl0

add atm=0 channel=1
```

3. Configure PPP for PPPoA

Create your PPPoA link, and define the username and password needed for Internet access. This is provided by your Internet Service Provider (ISP).

```
create ppp=0 over=atm0.1 echo=10 lqr=off bap=off idle=off

set ppp=0 username="branch office 1" password=branch1 iprequest=off
```

Note that this interface needs a permanent IP address because this branch office allows incoming roaming VPN client connections. The clients can only target a known, unchanging address.

4. Configure IP

Enable IP

```
enable ip
```

Define the vlan1 interface address. This VLAN connects the router to the branch office LAN.

```
add ip int=vlan1 ip=192.168.141.254
```

Define the fixed IP address of the ADSL PPP interface.

```
add ip int=ppp0 ip=222.222.222.1
```

Add a default route out the ADSL PPP interface. When using PPP, it is valid to define a null value next hop.

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

If desired, set up the router as a DHCP server for the branch office 1 LAN.

```
create dhcp policy=branch1 lease=7200

add dhcp policy=branch1 rou=192.168.141.254

add dhcp policy=branch1 subn=255.255.255.0

create dhcp range=branch1_hosts poli=branch1 ip=192.168.141.16 num=32

ena dhcp
```

5. Configure remote management access, if desired

If you need remote management access, we strongly recommend that you use Secure Shell (SSH). You should not telnet to a secure gateway.

To configure SSH, define appropriate RSA encryption keys, then enable the SSH server.

```
create enco key=2 type=rsa length=1024 description="host key"
    format=ssh

create enco key=3 type=rsa length=768 description="server key"
    format=ssh

enable ssh server serverkey=3 hostkey=2
```

Enable the user who connects via SSH to log in as secoff, by adding the secoff user as an SSH user. Also, you may choose to restrict access so that it is only permitted from particular addresses.

```
add ssh user=secoff password=<secoff-password>
    ipaddress=<trusted-remote-ip-address>
    mask=<subnet-mask-of-trusted-hosts>

disable telnet server
```

Secure Shell is a more secure, encrypted method of remote management access than telnet. If you need to use telnet, even though it is insecure, you should restrict access by defining remote security officers (RSOs). RSO definitions specify trusted remote addresses for security officer users.

```
add user rso ip=<ipadd>[-<ipadd>]

enable user rso

enable telnet server
```

6. Capture status information remotely, if desired

If desired, set the router to send log messages to a syslog server.

```
create log output=2 destination=syslog server=<syslog-server-address>
    syslogformat=extended

add log out=2 filter=1 sev=>3
```

If desired, you can configure SNMP to inform you or your service provider of network events, such as the LAN interface of the router going down. We recommend SNMPv3 for security reasons. For details, see *How To Configure SNMPv3 On Allied Telesis Routers and Managed Layer 3 Switches*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

7. Configure dynamic PPP over L2TP connections

You need to configure dynamic PPP over L2TP to accept incoming Windows VPN client connections.

Create an IP pool to allocate unique internal payload addresses to incoming VPN clients.

```
create ip pool=roaming ip=192.168.144.1-192.168.144.50
```

Define a PPP template. This defines authentication and uses the IP pool of addresses.

```
create ppp template=1

set ppp template=1 bap=off ippool=roaming authentication=chap echo=10
   lqr=off
```

Configure L2TP. When the router successfully negotiates an L2TP tunnel connection from any remote peer, it then creates a PPP interface over that tunnel, using the PPP parameters defined by the PPP template.

```
enable l2tp

enable l2tp server=both

add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
```

Add your approved roaming VPN client usernames.

```
add user=roaming2 pass=roaming2 lo=no telnet=no
```

If desired, you can instead use a RADIUS authentication server.

```
add radius server=<radius-server-address> secret=<secret-key>
```

8. Check feature licences

Check that you have a 3DES feature licence for the ISAKMP policies.

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor.

If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

9. Configure the VPNs for connecting to headquarters and roaming clients

Enable IPsec

```
enable ipsec
```

In this example, IPsec SA specifications propose:

- ISAKMP as the key management protocol
- ESP as the IPsec protocol

- (for site-to-site VPNs) 3DESOUTER as the encryption algorithm for ESP
- (for site-to-site VPNs) SHA as the hashing algorithm for ESP authentication
- (for roaming client VPNs) four possible variants of VPN encryption, for added flexibility. We propose the most secure option first.

Create an SA specification for the headquarters office site-to-site VPN. This SA specification uses tunnel mode by default.

```
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
```

Create a group of SA specifications for the roaming VPN clients. These SA specifications use IPsec transport mode for Windows VPN interoperability. Multiple specifications allow IPsec to negotiate different levels of encryption to match what your version of the VPN client provides.

```
create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=sha
   mod=transport

create ipsec sas=3 key=isakmp prot=esp enc=3desouter hasha=md5
   mod=transport

create ipsec sas=4 key=isakmp prot=esp enc=des hasha=sha mod=transport

create ipsec sas=5 key=isakmp prot=esp enc=des hasha=md5 mod=transport
```

Create two IPsec bundles, one for the headquarters router VPN and one for the roaming VPN clients.

```
create ipsec bund=1 key=isakmp string="1"

create ipsec bund=2 key=isakmp string="2 or 3 or 4 or 5"
```

Create IPsec policies to bypass IPsec for ISAKMP messages and the “port floated” key exchange that NAT-T uses.

```
create ipsec pol=isakmp int=ppp0 ac=permit lp=500 rp=500

create ipsec pol=isakmp_float int=ppp0 ac=permit lp=4500
```

Create an IPsec policy for the VPN traffic between headquarters and branch office 1. Identify the traffic by its local and remote addresses—in this example the subnet used on the LAN at branch office 1 (local) is 192.168.141.0/24. Note that the remote address selector is wider than the headquarter’s LAN; in fact, we cover all site subnets with this supernet.

```
create ipsec pol=hq int=ppp0 ac=ipsec key=isakmp bund=1
   peer=200.200.200.1 isa=hq lad=192.168.141.0 lma=255.255.255.0
   rad=192.168.0.0 rma=255.255.0.0
```

Create another IPsec policy for roaming VPN clients to access headquarters. Identify the traffic by the L2TP port (UDP traffic to port 1701). This policy uses **peeraddress=any**. The **any** option allows simultaneous VPN clients to be set up under the policy.

```
create ipsec pol=roaming int=ppp0 ac=ipsec key=isakmp bund=2 peer=any
   isa=roaming lp=1701 tra=udp
```

Create another IPsec policy for direct Internet traffic from the headquarters LAN to the Internet, such as web browsing.

```
create ipsec pol=internet int=ppp0 ac=permit
```

Note: The order of the IPsec policies is important. The Internet permit policy must be last.

Create your ISAKMP pre-shared key. This key is used when initiating your VPN during phase one ISAKMP exchanges with your VPN peers. Share the value of this pre-shared key with all VPN peers that use it—in this example, the roaming VPN clients and the headquarters router. The router only uses this key during phase one ISAKMP exchanges.

```
create enco key=1 type=general value=<alphanumeric-preshared-key>
```

Enable ISAKMP.

```
ena isa
```

Like the headquarters policy (see comments on page 12) this example uses separate ISAKMP policies for each peer.

Create an ISAKMP policy for the VPN to headquarters, with a fixed address. Use ISAKMP heartbeats, which allow ISAKMP to clear SAs if either end of the link resets.

```
create isakmp pol=hq pe=200.200.200.1 sendd=true key=1 heart=both
   localid=branch1 encalg=3des2key
```

Create an ISAKMP policy for roaming VPN clients, with **peer=any** because the peers have dynamic addresses. Note that you cannot use heartbeats with Windows peers. We recommend that you enable NAT-T, because the roaming VPN clients will sometimes need to connect through a NAT-T gateway.

```
create isakmp pol=roaming pe=any key=1 sendd=true sendi=on natt=true
   localid=branch1
```

The roaming policy uses the same key as the policy for the headquarters VPN. If you want to, you can instead generate a unique pre-shared key to use with the roaming clients, and attach it to the roaming policy.

10. Configure the firewall's basic settings

Enable the firewall and create a firewall policy.

```
enable firewall

create firewall policy=branch1

enable firewall policy=branch1 icmp_f=all
```

Specify the LAN-facing interface of the router as a private (trusted) interface on the firewall.

```
add firewall policy=branch1 int=vlan1 type=private
```

Specify the Internet-facing interface of the router as a public (not trusted) interface on the firewall.

```
add firewall policy=branch1 int=ppp0 type=public
```

Define a firewall dynamic definition to enable dynamically created interfaces to participate in the firewall. In this case, the definition provides for the dynamic PPP over L2TP interfaces that incoming Windows VPN connections use. In other words, when the router dynamically creates PPP interfaces over the L2TP connections from the roaming PC clients, the router automatically adds these dynamic interfaces as private interfaces on the firewall. The router can trust traffic arriving on the dynamic interfaces because—in this example configuration—it can only come from an authenticated and encrypted VPN connection.

```
create firewall policy=branch1 dynamic=roaming

add firewall policy=branch1 dynamic=roaming user=any

add firewall policy=branch1 int=dyn-roaming type=private
```

Define NAT definitions to use when traffic from the local LAN accesses the Internet and to allow Internet access for remote VPN client users.

```
add firewall policy=branch1 nat=enhanced int=vlan1 gblin=ppp0

add firewall policy=branch1 nat=enhanced int=dyn-roaming gblin=ppp0
```

Note: Windows VPN client default behaviour does not support "split tunnelling". This means that when the Windows VPN tunnel is up, all traffic passes through it, whether the traffic is destined for the branch office LAN or for Internet surfing destinations. Therefore, we suggest you define the second NAT above, to allow clients to access the Internet via the branch office router when their VPN connection is up.

11. Configure the firewall's access rules

Create a rule to allow incoming ISAKMP negotiation messages to pass through the firewall.

```
add firewall policy=branch1 ru=1 ac=allo int=ppp0 prot=udp po=500
    ip=222.222.222.1 gblip=222.222.222.1 gblp=500
```

Create a rule to support NAT-T. If a NAT gateway is detected in the VPN path, NAT-T "port floats" IKE to port 4500, and also encapsulates IPsec inside UDP headers to the same port. Therefore, UDP traffic to port 4500 must be allowed to pass through the firewall.

```
add firewall policy=branch1 ru=2 ac=allo int=ppp0 prot=udp po=4500
    ip=222.222.222.1 gblip=222.222.222.1 gblp=4500
```

Create a rule for the roaming VPN clients. Windows VPN client uses L2TP (UDP to port 1701) encapsulated inside IPsec. This rule allows L2TP traffic through the firewall if it originally arrived at the router encapsulated in IPsec (and was decapsulated by the IPsec process before it passed to the firewall).

```
add firewall policy=branch1 ru=3 ac=allo int=ppp0 prot=udp po=1701
    ip=222.222.222.1 gblip=222.222.222.1 gblp=1701 enc=ips
```

Create a pair of rules to allow office-to-office payload traffic to pass through the firewall without applying NAT. This traffic must bypass NAT so that the traffic matches subsequent IPsec policy address selectors. You need two rules—one for the public interface and one for the private interface—so that office-to-office payload traffic bypasses NAT regardless of which side initiated the session.

The rule for the public interface uses **encapsulation=ipsec** to identify incoming VPN traffic—decrypted payload data that came from the IPsec module.

```
add firewall policy=branch1 ru=4 ac=non int=ppp0 prot=all enc=ips
```

The rule for the private interface uses both source and destination addresses to identify outgoing VPN traffic.

```
add firewall policy=branch1 ru=5 ac=non int=vlan1 prot=all
   ip=192.168.141.1-192.168.141.254 rem=192.168.140.0-192.168.142.254
```

If you configured SSH (recommended), create a rule to allow SSH traffic to pass through the firewall.

```
add firewall policy=branch1 ru=6 ac=allo int=ppp0 prot=tcp po=22
   ip=222.222.222.1 gblip=222.222.222.1 gblp=22
```

If you instead stayed with telnet (not recommended) and configured RSOs, create a rule to allow telnet traffic to pass through the firewall.

```
add firewall policy=branch1 ru=7 ac=allo int=ppp0 prot=tcp po=23
   ip=222.222.222.1 gblip=222.222.222.1 gblp=23
```

12. Save your configuration

It is important to save your configuration when you finish, to preserve the configuration over any power cuts.

```
create conf=<your-file.cfg>
```

This is particularly important in security configurations because it preserves the security officer definition. Without this, regaining configuration access would destroy encryption information such as keys.

Once you have saved the configuration to a file, specify that file as the configuration script to use when the router boots up.

```
set config=<your-file.cfg>
```

How to configure the AR440S router at branch office 2

Before you begin to configure your router, ensure that it is running the appropriate software release, patch and GUI files and has no configuration.

```
set inst=pref rel=<rel-file> pat=<patch-file> gui=<gui-file>

set conf=none

disable system security

restart reboot
```

Note: A software QoS extension to this configuration, to prioritise VoIP traffic over the VPNs, is available in "How to prioritise outgoing VoIP traffic from the headquarters router" on page 31.

1. Configure general system and user settings

Name the router

```
set system name=Branch2
```

Define a security officer.

```
add user=secoff pass=<your-secoff-password> priv=securityofficer
   lo=yes telnet=yes
```

Do not forget your “secoff” password.

Enable security mode so that VPN keys are stored securely, and other security features are enabled.

```
enable system security
```

Once security mode is enabled, you need to log in as a security officer to enter most configuration-altering commands.

```
login secoff

password: <your-secoff-password>
```

It is important to keep this security officer username and password secure, and to consider proper handover of it in the event of IT staff changes.

Also, we recommend you leave a “manager” privilege user defined because this may provide backup access if the security officer password is lost. Do not leave the manager password at the factory default—change it to a password in keeping with your company's security policy.

```
set user=manager password=<your-company-policy-password>
```

When security mode is enabled, router configuration access times out after inactivity to prevent unauthorised access. The default timeout is 60 seconds, but you may temporarily raise it to 600 seconds if desired.

```
set user securedelay=600
```

2. Configure ADSL for internet access

Create your Asymmetric Digital Subscriber Line (ADSL) connection. Asynchronous Transfer Mode (ATM) is always used over ADSL.

```
enable adsl=0

create atm=0 over=adsl0

add atm=0 channel=1
```

Branch 2 uses PPPoEoA (PPP over virtual ethernet over ATM). Create the virtual ethernet over ATM.

```
create eth=0 over=atm0.1
```

3. Configure PPP for PPPoE

Create your PPPoE link, and define the username and password needed for Internet access. This is provided by your Internet Service Provider (ISP). Use **iprequest=on so** that the interface obtains its address dynamically from the ISP—this office has no incoming roaming VPN clients so does not need a fixed address.

```
create ppp=0 over=eth0-any echo=10 lqr=off bap=off idle=off

set ppp=0 iprequest=on username="branch office 2" password=branch2
```

4. Configure IP

Enable IP

```
enable ip
```

Define the vlan1 interface address. This VLAN connects the router to the branch office LAN.

```
add ip int=vlan1 ip=192.168.142.254
```

The interface ppp0 (over virtual ethernet and ATM/ADSL) provides the Internet connection interface. Enable IP remote assignment, to allow your ISP to dynamically assign an IP address to ppp0.

```
enable ip remote
```

Configure a temporary null address.

```
add ip int=ppp0 ip=0.0.0.0
```

Add a default route out the ADSL PPP interface. When using PPP, it is valid to define a null value next hop.

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

If desired, set up the router as a DHCP server for the branch office 2 LAN.

```
create dhcp policy=branch2 lease=7200

add dhcp policy=branch2 rou=192.168.142.254

add dhcp policy=branch2 subn=255.255.255.0

create dhcp range=branch2_hosts poli=branch2 ip=192.168.142.16 num=32

ena dhcp
```

5. Configure remote management access, if desired

If you need remote management access, we strongly recommend that you use Secure Shell (SSH). You should not telnet to a secure gateway.

To configure SSH, define appropriate RSA encryption keys, then enable the SSH server.

```
create enco key=2 type=rsa length=1024 description="host key"
   format=ssh

create enco key=3 type=rsa length=768 description="server key"
   format=ssh

enable ssh server serverkey=3 hostkey=2
```

Enable the user who connects via SSH to log in as secoff, by adding the secoff user as an SSH user. Also, you may choose to restrict access so that it is only permitted from particular addresses.

```
add ssh user=secoff password=<secoff-password>
   ipaddress=<trusted-remote-ip-address>
   mask=<subnet-mask-of-trusted-hosts>

disable telnet server
```

Secure Shell is a more secure, encrypted method of remote management access than telnet. If you need to use telnet, even though it is insecure, you should restrict access by defining remote security officers (RSOs). RSO definitions specify trusted remote addresses for security officer users.

```
add user rso ip=<ipadd>[-<ipadd>]

enable user rso

enable telnet server
```

6. Capture status information remotely, if desired

If desired, set the router to send log messages to a syslog server.

```
create log output=2 destination=syslog server=<syslog-server-address>
   syslogformat=extended

add log out=2 filter=1 sev=>3
```

If desired, you can configure SNMP to inform you or your service provider of network events, such as the LAN interface of the router going down. We recommend SNMPv3 for security reasons. For details, see *How To Configure SNMPv3 On Allied Telesis Routers and Managed Layer 3 Switches*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

7. Check feature licences

Check that you have a 3DES feature licence for the ISAKMP policy.

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor.

If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

8. Configure the VPNs for connecting to the headquarters office

Enable IPsec

```
enable ipsec
```

In this example, IPsec SA specification proposes:

- ISAKMP as the key management protocol
- ESP as the IPsec protocol
- 3DES as the encryption algorithm for ESP
- SHA as the hashing algorithm for ESP authentication

Create an SA specification for the headquarters office site-to-site VPN. This SA specification uses tunnel mode by default.

```
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
```

Note that the branch office 2 router has no connections from roaming VPN clients so does not need SA specifications for them.

Create an IPsec bundle for the SA specification.

```
create ipsec bund=1 key=isakmp string="1"
```

Create an IPsec policy to permit ISAKMP messages to bypass IPsec.

```
create ipsec pol=isakmp int=ppp0 ac=permit lp=500 rp=500
```

Create an IPsec policy for the VPN traffic between headquarters and branch office 2. Identify the traffic by its local and remote addresses—in this example the subnet used on the LAN at branch office 2 (local) is 192.168.142.0/24 so use that as the local address selector. However, define a wider remote address selector, to allow for other incoming VPN traffic via headquarters.

```
create ipsec pol=hq int=ppp0 ac=ipsec key=isakmp bund=1
   peer=200.200.200.1 isa=hq lad=192.168.142.0 lma=255.255.255.0
   rad=192.168.0.0 rma=255.255.0.0
```

Create another IPsec policy for direct Internet traffic from the headquarters LAN to the Internet, such as web browsing.

```
        create ipsec pol=internet int=ppp0 ac=permit
```

Note: The order of the IPsec policies is important. The Internet permit policy must be last.

Create your ISAKMP pre-shared key. This key is used when initiating your VPN during phase one ISAKMP exchanges with your VPN peers. Share the value of this pre-shared key with all VPN peers that use it—in this example, the headquarters router. The router only uses this key during phase one ISAKMP exchanges.

```
        create enco key=1 type=general value=<alphanumeric-preshared-key>
```

Enable ISAKMP.

```
        enable isakmp
```

Create an ISAKMP policy for the VPN to headquarters. Use ISAKMP heartbeats, which allow ISAKMP to clear SAs if either end of the link resets.

```
        create isakmp pol=hq pe=200.200.200.1 sendd=true key=1 heart=both
            localid=branch2 encalg=3des2key
```

9. Configure the firewall's basic settings

Enable the firewall and create a firewall policy.

```
        enable firewall

        create firewall policy=branch2

        enable firewall policy=branch2 icmp_f=all
```

Specify the LAN-facing interface of the router as a private (trusted) interface on the firewall.

```
        add firewall policy=branch2 int=vlan1 type=private
```

Specify the Internet-facing interface of the router as a public (not trusted) interface on the firewall.

```
        add firewall policy=branch2 int=ppp0 type=public
```

Define a NAT definition to use when traffic from the local LAN accesses the Internet.

```
        add firewall policy=branch2 nat=enhanced int=vlan1 gblin=ppp0
```

10. Configure the firewall's access rules

Create a rule to allow incoming ISAKMP negotiation messages to pass through the firewall. This rule specifies 0.0.0.0 as the global IP address because the PPP address of branch office 2 is dynamically assigned. The rule uses the LAN address to identify matching traffic.

```
        add firewall policy=branch2 ru=1 ac=allo int=ppp0 prot=udp po=500
            ip=192.168.142.254 gblip=0.0.0.0 gblp=500
```

Branch office 2 does not need rule 3 that the other sites have, because branch office 2 has no roaming VPN client connections.

Create a pair of rules to allow office-to-office payload traffic to pass through the firewall without applying NAT. This traffic must bypass NAT so that the traffic matches subsequent IPsec policy address selectors. You need two rules—one for the public interface and one for the private interface—so that office-to-office payload traffic bypasses NAT regardless of which side initiated the session.

The rule for the public interface uses **encapsulation=ipsec** to identify incoming VPN traffic—decrypted payload data that came from the IPsec module.

```
add firewall policy=branch2 ru=4 ac=non int=ppp0 prot=all enc=ips
```

The rule for the private interface uses both source and destination addresses to identify outgoing VPN traffic.

```
add firewall policy=branch2 ru=5 ac=non int=vlan1 prot=all
   ip=192.168.142.1-192.168.142.254 rem=192.168.140.0-192.168.142.254
```

If you configured SSH (recommended), create a rule to allow SSH traffic to pass through the firewall.

```
add firewall policy=branch2 ru=6 ac=allo int=ppp0 prot=tcp po=22
   ip=192.168.142.254 gblip=0.0.0.0 gblp=22
```

If you instead stayed with telnet (not recommended) and configured RSOs, create a rule to allow telnet traffic to pass through the firewall.

```
add firewall policy=branch2 ru=7 ac=allo int=ppp0 prot=tcp po=23
   ip=192.168.142.254 gblip=0.0.0.0 gblp=23
```

11. Save your configuration

It is important to save your configuration when you finish, to preserve the configuration over any power cuts.

```
create conf=<your-file.cfg>
```

This is particularly important in security configurations because it preserves the security officer definition. Without this, regaining configuration access would destroy encryption information such as keys.

Once you have saved the configuration to a file, specify that file as the configuration script to use when the router boots up.

```
set config=<your-file.cfg>
```

How to make voice traffic high priority

This is an optional enhancement to the configuration of the routers. It prioritises outgoing voice traffic higher than other outgoing traffic on each VPN, to maximise call quality.

Use the configuration in this section if you expect your VPN client or branch office users will be using VoIP over a VPN. The configuration consists of the following sections:

- "How to prioritise outgoing VoIP traffic from the headquarters router"
- "How to prioritise outgoing VoIP traffic from the branch office 1 router"
- "How to prioritise outgoing VoIP traffic from the branch office 2 router"

This enhancement prioritises outgoing voice traffic rather than incoming voice traffic, because the link to the ISP is the most likely point of congestion.

We recommend you configure prioritisation on both peers in each VPN, not just on the headquarters router, because the link from either peer to its ISP could become a point of congestion.

Note: This enhancement only prioritises outgoing VoIP traffic at the routers you configure it on. Of course, you cannot control the quality of service on routers in the Internet, such as your ISP's routers.

Classifying VoIP traffic

In the following configurations, the router classifies voice traffic by checking packets' IP DSCP values. If the originating VoIP appliance does not mark packets with a DSCP value, you can instead select the voice traffic by:

- classifying on the range of destination ports that the appliance uses for RTP (Real Time Protocol—the protocol that carries voice data), or
- use the Dynamic Application Recognition (DAR) system, which dynamically determines the ports

If you also need to classify the signalling traffic (call setup etc) and the signalling traffic is not DSCP-marked, then create classifiers for the appropriate ports. For example, H.323 signalling traffic uses TCP ports 1720 and 1721, and SIP uses UDP port 5060. To create classifiers for H.323 signalling packets, use the following commands:

```
create classifier=<id> tcpd=1720

create classifier=<id> tcpd=1721
```

For more information, including information about DAR, see the following:

- the “Software Quality of Service (QoS)” and “Generic Packet Classifier” chapters of the *Software Reference*
- *How To Configure Software QoS For Some Specific Customer Scenarios*. This How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

How to prioritise outgoing VoIP traffic from the headquarters router

Add the following steps after step 9 on page 14.

1. Create classifiers

First, classify the VoIP traffic. In many deployments of VoIP, the originating VoIP appliance marks VoIP packets with a DSCP value. In this example, it marks both VoIP traffic and VoIP signalling packets with DSCP 48.

```
create classifier=48 ipds=48
```

2. Reduce the MTU

VoIP data packets are small. They can be significantly delayed by big packets on the WAN port, especially on slow links. Therefore, you may find it helpful to reduce the MTU for all packets on the WAN port, for example, to 256 bytes.

```
set int=eth0 mtu=256
```

You also need to make sure that **all** large packets are fragmented, even if they were previously set to not be fragmented.

```
set int=eth0 frag=yes
```

3. Set up software QoS to ensure VoIP traffic has high priority

Enable software QoS (SQoS) and create an SQoS traffic class. This traffic class tags the classified traffic as high priority on the interface queue. Also define a small queue size, which is optimal for VoIP traffic.

```
ena sqos

cre sqos tr=1 prio=15 maxq=10
```

Create an SQoS policy and assign the traffic class to this policy. To make SQoS prioritisation effective, define a suitable virtual bandwidth for the interface being used. As the bandwidth limit is approached, SQoS can drop packets in a controlled manner and let high priority packets pass first.

```
cre sqos policy=1 virt=120kbps

add sqos policy=1 tr=1

add sqos tr=1 classifier=48
```

Note that this step has not yet applied the policy to interfaces. For site-to-site VPNs, the next step applies the policy directly to the tunnels. For roaming clients, the interfaces are dynamically-created for incoming connections, so step 5 on page 32 defines triggers to automatically apply the policy when connections establish.

4. For site-to-site VPNs, apply the SQoS policy to the tunnels

Apply the policy to the VPN between headquarters and branch office 1.

```
set sqos interface=ipsec-branch1 tunnelpolicy=1
```

Apply the policy to the VPN between headquarters and branch office 2.

```
set sqos interface=ipsec-branch2 tunnelpolicy=1
```

5. For roaming clients, use triggers to apply SQoS to dynamic interfaces

This example creates four triggers, which allows for up to four simultaneous roaming client VPNs. You can scale this to the correct number for your network.

Create the following scripts as text files on the router.

script name	script contents
ppp0up.scp	set sqos int=ppp0 outpolicy=1
ppp1up.scp	set sqos int=ppp1 outpolicy=1
ppp2up.scp	set sqos int=ppp2 outpolicy=1
ppp3up.scp	set sqos int=ppp3 outpolicy=1

Create triggers to run the appropriate script when the interface comes up.

```
enable trigger
create trigger=1 interface=ppp0 event=up cp=ipcp script=ppp0up.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=ppp1up.scp
create trigger=3 interface=ppp0 event=up cp=ipcp script=ppp2up.scp
create trigger=4 interface=ppp0 event=up cp=ipcp script=ppp3up.scp
```

6. For roaming clients, set L2TP TOS reflection

You need TOS (type of service) reflection so that DSCP marked VoIP packets can be classified for prioritisation at the PPP level. Unless you already turned on TOS reflection when you configured L2TP in step 5 on page 10, delete your existing L2TP entry and add it again.

```
delete l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1 tos=on
```

7. Save your configuration

```
create conf=<your-file.cfg>
set config=<your-file.cfg>
```

How to prioritise outgoing VoIP traffic from the branch office 1 router

Add the following steps after step 11 on page 22.

1. Create classifiers

In this example, the originating VoIP appliance has marked VoIP traffic and VoIP signalling packets with DSCP 48.

```
create classifier=48 ipds=48
```

2. Reduce the MTU

VoIP data packets are small. They can be significantly delayed by big packets on the WAN port, especially on slow links. Therefore, you may find it helpful to reduce the MTU for all packets on the WAN port, for example, to 256 bytes.

```
set int=ppp0 mtu=256
```

You also need to make sure that **all** large packets are fragmented, even if they were previously set to not be fragmented.

```
set int=ppp0 frag=yes
```

3. Set up software QoS to ensure VoIP traffic has high priority

Enable software QoS (SQoS), create an SQoS traffic class, and define a small queue size.

```
ena sqos
cre sqos tr=1 prio=15 maxq=10
```

Create an SQoS policy, assign the traffic class to this policy, and define a suitable virtual bandwidth for the interface being used.

```
cre sqos policy=1 virt=120kbps
add sqos policy=1 tr=1
add sqos tr=1 classifier=48
```

4. For the site-to-site VPN, apply the SQoS policy to the tunnel

Apply the policy to the VPN between branch office 1 and headquarters.

```
set sqos interface=ipsec-hq tunnelpolicy=1
```

5. For roaming clients, use triggers to apply SQoS to dynamic interfaces

This example creates four triggers, which allows for up to four simultaneous roaming client VPNs. You can scale this to the correct number for your network.

Create the following scripts as text files on the router.

script name	script contents
ppp0up.scp	set sqos int=ppp0 outpolicy=1
ppp1up.scp	set sqos int=ppp1 outpolicy=1
ppp2up.scp	set sqos int=ppp2 outpolicy=1
ppp3up.scp	set sqos int=ppp3 outpolicy=1

Create triggers to run the appropriate script when the interface comes up.

```
enable trigger
create trigger=1 interface=ppp0 event=up cp=ipcp script=ppp0up.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=ppp1up.scp
create trigger=3 interface=ppp0 event=up cp=ipcp script=ppp2up.scp
create trigger=4 interface=ppp0 event=up cp=ipcp script=ppp3up.scp
```

6. For roaming clients, set L2TP TOS reflection

You need TOS (type of service) reflection so that DSCP marked VoIP packets can be classified for prioritisation at the PPP level. Unless you already turned on TOS reflection when you configured L2TP in step 7 on page 19, delete your existing L2TP entry and add it again.

```
delete l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1 tos=on
```

7. Save your configuration

```
create conf=<your-file.cfg>
set config=<your-file.cfg>
```

How to prioritise outgoing VoIP traffic from the branch office 2 router

Add the following steps after step 11 on page 22.

1. Create classifiers

In this example, the originating VoIP appliance has marked VoIP traffic and VoIP control packets with DSCP 48.

```
create classifier=48 ipds=48
```

2. Reduce the MTU

VoIP data packets are small. They can be significantly delayed by big packets on the WAN port, especially on slow links. Therefore, you may find it helpful to reduce the MTU for all packets on the WAN port, for example, to 256 bytes.

```
set int=ppp0 mtu=256
```

You also need to make sure that **all** large packets are fragmented, even if they were previously set to not be fragmented.

```
set int=ppp0 frag=yes
```

3. Set up software QoS to ensure VoIP traffic has high priority

Enable software QoS (SQoS), create an SQoS traffic class, and define a small queue size.

```
ena sqos
cre sqos tr=1 prio=15 maxq=10
```

Create an SQoS policy, assign the traffic class to this policy, and define a suitable virtual bandwidth for the interface being used.

```
cre sqos policy=1 virt=120kbps
add sqos policy=1 tr=1
add sqos tr=1 classifier=48
```

4. Apply the SQoS policy to the tunnel

Apply the policy to the VPN between branch office 2 and headquarters.

```
set sqos interface=ipsec-hq tunnelpolicy=1
```

5. Save your configuration

```
create conf=<your-file.cfg>
set config=<your-file.cfg>
```

How to test your VPN solution

If the following tests show that your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

Check the LANs are reachable

The simplest way to test a tunnel is to ping from one LAN to the other.

From a PC attached to one peer, ping a PC attached to the other peer. For example, you can test the VPN between branch office 1 and headquarters by pinging any PC in the branch office 1 LAN from any PC in the headquarters LAN. If a PC in the branch office 1 LAN has an address of 192.168.141.1, that means using the following command at the command prompt on a PC at headquarters:

```
ping 192.168.141.1
```

If a Microsoft Windows PC's IP address was assigned dynamically, you can find out what it is by using the following command at the command prompt:

```
ipconfig
```

Check traffic goes through the VPN

To tell if traffic passes through the tunnel, perform a traceroute from one LAN to the other—so from a PC attached to one peer, perform a traceroute to a PC attached to the other peer. For example, if a PC in the branch office 1 LAN has an address of 192.168.141.1, that means using the following command at the command prompt on a (Windows) PC at headquarters:

```
tracert 192.168.141.1
```

If traffic goes through the tunnel, the traceroute may display IP addresses from one or both peers' private networks and public interfaces. If it shows other public IP addresses, then traffic is not passing through the tunnel.

Configuration scripts for headquarters and branch offices

This section provides script-only versions of the three configurations described earlier in this document. Scripts can provide a quicker way to configure your routers, through pre-editing and downloading using TFTP or ZMODEM.

You can copy and paste the scripts below to an editor on your PC, modify addresses, passwords and any other requirements for all your individual sites, and then use TFTP or ZMODEM to transfer the files to your routers.

Please refer to the “Managing Configuration Files and Software Versions” chapter in the *Software Reference* for more information about TFTP and ZMODEM.

Before you use these scripts

You need to do the following aspects of the security configuration by entering commands in the command line instead of adding them to the scripts:

- creating a security officer (this needs to be in the script as well)

```
add user=secoff pass=<your-secoff-password> priv=securityofficer
   lo=yes telnet=yes
```

- enabling system security

```
enable system security
```

- logging in as security officer

```
login secoff
```

- enabling the 3DES feature licence if it is not factory-enabled

```
enable feature=3des pass=<licence-number>
```

- defining encryption keys for SSH and ISAKMP.

```
cre enco key=1 type=general value=<alphanumeric-preshared-key>

cre enco key=2 type=rsa length=1024 desc="host key" format=ssh

cre enco key=3 type=rsa length=768 desc="server key" format=ssh
```

Color coding

For your convenience, the scripts are color-coded:

🟩 headquarters 🟧 branch office 1 🟦 branch office 2

Headquarters

Headquarters VPN access concentrator's configuration

```
# System configuration

set system name=HQ

# User configuration

set user securedelay=600

# Add your approved roaming VPN client usernames.

add user=roaming1 pass=roaming1 lo=no telnet=no

add user=roaming2 pass=roaming2 lo=no telnet=no

add user=roaming3 pass=roaming3 lo=no telnet=no

add user=roaming4 pass=roaming4 lo=no telnet=no

# Define a security officer.

add user=secoff pass=<your-secoff-password> priv=securityofficer
  lo=yes telnet=yes

# Change the manager privilege user’s password.

set user=manager password=<your-password>

# RADIUS configuration

# If desired, add a RADIUS authentication server for authenticating
# users.

add radius server=<radius-server-address> secret=<secret-key>

# PPP template configuration

# Create a template to use for incoming roaming Windows VPN client
# connections. This defines authentication and associates the IP pool
# of addresses that are allocated to clients.

create ppp template=1

set ppp template=1 bap=off ippool=roaming authentication=chap echo=10
  lqr=off

# L2TP configuration

# Configure an L2TP server to accept incoming roaming Windows VPN
# client connections

enable l2tp

enable l2tp server=both

add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1 tos=on

# IP configuration

enable ip

add ip int=vlan1 ip=192.168.140.254

# Configure eth0 for connecting to the Internet with a fixed address.

add ip int=eth0 ip=200.200.200.1

add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=200.200.200.254

# Create an IP pool to allocate unique internal payload addresses to
# incoming VPN clients.

create ip pool=roaming ip=192.168.143.1-192.168.143.50
```

```
# DHCP configuration

# If desired, use the router as a DHCP server.

create dhcp poli=hq lease=7200

add dhcp poli=hq rou=192.168.140.254

add dhcp poli=hq subn=255.255.255.0

create dhcp range=hq_hosts poli=hq ip=192.168.140.16 num=32

ena dhcp

# SSH configuration

# You should not telnet to a secure gateway, so set up Secure Shell
# for remote management. This requires encryption keys - see
# "Before you start" on page 7.

# Enable the SSH server.

enable ssh server serverkey=3 hostkey=2

# Enable the user who connects via SSH to log in as secoff, by adding
# the secoff user as an SSH user. If desired, also restrict access so
# that it is only permitted from particular addresses.

add ssh user=secoff password=<secoff-password>
  ipaddress=<trusted-remote-ip-address>
  mask=<desired-subnet-mask-of-trusted-hosts>

disable telnet server

# As the commands above show, we strongly recommend SSH instead of
# telnet. However, if you choose to use telnet, create RSO users
# (remote security officers) and define the IP addresses that these
# users may connect from.

# add user rso ip=<ipadd>[-<ipadd>]

# enable user rso

# enable telnet server

# Log configuration

# If desired, forward router log entries to a UNIX-style syslog
# server.

create log output=2 destination=syslog
  server=<your-local-syslog-server-address> syslogformat=extended

add log out=2 filter=1 sev=>3

# IPSEC configuration

# Create an SA specification for the site-to-site VPN. This SA
# specification uses tunnel mode by default.

create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha
```

```
# Create a group of SA specifications for the roaming VPN clients.
# These SA specifications use IPsec transport mode.

create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=sha
  mod=transport

create ipsec sas=3 key=isakmp prot=esp enc=3desouter hasha=md5
  mod=transport

create ipsec sas=4 key=isakmp prot=esp enc=des hasha=sha
  mod=transport

create ipsec sas=5 key=isakmp prot=esp enc=des hasha=md5
  mod=transport

create ipsec bund=1 key=isakmp string="1"

create ipsec bund=2 key=isakmp string="2 or 3 or 4 or 5"

# Create IPsec policies to bypass IPsec for ISAKMP messages and the
# "port floated" key exchange that NAT-T uses.

create ipsec pol=isakmp int=eth0 ac=permit

set ipsec pol=isakmp lp=500 rp=500

create ipsec pol=isakmp_float int=eth0 ac=permit

set ipsec pol=isakmp_float lp=4500

# Create an IPsec policy for branch 1 to headquarters VPN traffic.

create ipsec pol=branch1 int=eth0 ac=ipsec key=isakmp isa=branch1
  bund=1 peer=222.222.222.1

set ipsec pol=branch1 lad=192.168.0.0 lma=255.255.0.0
  rad=192.168.141.0 rma=255.255.255.0

# Create another IPsec policy for branch 2 to headquarters VPN
# traffic.

create ipsec pol=branch2 int=eth0 ac=ipsec key=isakmp isa=branch2
  bund=1 peer=dynamic

set ipsec pol=branch2 lad=192.168.0.0 lma=255.255.0.0
  rad=192.168.142.0 rma=255.255.255.0

# Create another IPsec policy for roaming VPN clients. This policy
# uses the L2TP port to identify traffic.

create ipsec pol=roaming int=eth0 ac=ipsec key=isakmp bund=2 peer=any
  isa=roaming

set ipsec pol=roaming lp=1701 tra=udp

# Create another IPsec policy to allow for direct Internet access
# such as web browsing.

create ipsec pol=internet int=eth0 ac=permit

enable ipsec

# ISAKMP Configuration

create isakmp pol=branch1 pe=222.222.222.1 sendd=true key=1
  heart=both encalg=3des2key localid=hq

create isakmp pol=branch2 pe=any sendd=true key=1 heart=both
  encalg=3des2key localid=hq

create isakmp pol=roaming pe=any key=1

set isakmp pol=roaming sendd=true sendi=true natt=true localid=hq

enable isakmp
```

```
# FIREWALL configuration

enable firewall

create firewall policy=hq

enable firewall policy=hq icmp_f=all

# Define a firewall dynamic definition to work with dynamic
# interfaces. This provides for the dynamic PPP/L2TP interfaces that
# incoming Windows VPN connections use.

create firewall policy=hq dy=roaming

add firewall policy=hq dy=roaming user=any

# Specify the private and public interfaces. The roaming interface is
# private - you can trust it because it comes from an authenticated
# Windows VPN connection.

add firewall policy=hq int=dyn-roaming type=private

add firewall policy=hq int=vlan1 type=private

add firewall policy=hq int=eth0 type=public

# Create a NAT definition for traffic from the headquarters LAN to
# use when accessing the Internet.

add firewall poli=hq nat=enhanced int=vlan1 gblin=eth0

# Create another NAT definition for roaming VPN clients to use when
# accessing the Internet via the headquarters router.

add firewall poli=hq nat=enhanced int=dyn-roaming gblin=eth0

# Create a rule to allow incoming ISAKMP negotiation to pass through
# the firewall.

add firewall poli=hq ru=1 ac=allo int=eth0 prot=udp po=500
  ip=200.200.200.1 gblip=200.200.200.1 gblp=500

# Create a rule to support NAT-T. If there is a NAT gateway in the
# VPN path, NAT-T "port floats" IKE to port 4500, and also
# encapsulates IPsec inside the same port.

add firewall poli=hq ru=2 ac=allo int=eth0 prot=udp po=4500
  ip=200.200.200.1 gblip=200.200.200.1 gblp=4500

# Create a rule for the roaming VPN clients. Windows uses L2TP (port
# 1701) inside IPsec. This rule allows traffic that comes from IPsec
# and uses port 1701.

add firewall poli=hq ru=3 ac=allo int=eth0 prot=udp po=1701
  ip=200.200.200.1 gblip=200.200.200.1 gblp=1701 enc=ips

# Create a pair of rules to allow office-to-office payload traffic to
# pass through the firewall without applying NAT.
# The rule for the public interface uses encapsulation=ipsec to
# identify incoming VPN traffic.

add firewall poli=hq ru=4 ac=non int=eth0 prot=all enc=ips

# The rule for the private interface uses both source and destination
# addresses to identify outgoing VPN traffic.

add firewall poli=hq ru=5 ac=non int=vlan1 prot=all
  ip=192.168.140.1-192.168.140.254

set firewall poli=hq ru=5 rem=192.168.141.0-192.168.144.254
```

Headquarters

```
# If you configured SSH, create a rule for SSH traffic.

add firewall policy=hq ru=6 ac=allo int=eth0 prot=tcp po=22
  ip=200.200.200.1 gblip=200.200.200.1 gblp=22

# If you use telnet instead (not recommended), create a rule for it.
# add firewall policy=hq ru=7 ac=allo int=eth0 prot=tcp po=23
# ip=200.200.200.1 gblip=200.200.200.1 gblp=23

# INT configuration - if prioritising VoIP

set int=eth0 mtu=256

set int=eth0 frag=yes

# CLASSIFIER configuration - if prioritising VoIP

# Create a classifier to identify voice traffic (DSCP value 48 in
# this example).

create class=48 ipds=48

# Software QoS configuration - if prioritising VoIP

ena sqos

# Create a traffic class. This traffic class tags the classified
# traffic as high priority on the interface queue. Also,make the
# queue small - this is optimal for VoIP traffic.

cre sqos tr=1 prio=15 maxq=10

# Create a policy with a virtual bandwidth and assign the traffic
# class to this policy.

cre sqos poli=1 virt=120kbps

add sqos poli=1 tr=1

add sqos tr=1 class=48

set sqos interface=ipsec-branch1 tunnelpolicy=1

set sqos interface=ipsec-branch2 tunnelpolicy=1

# TRIGGER configuration - if prioritising VoIP

# Create triggers to apply SQoS to the dynamic PPP interfaces of up
# to four simultaneous roaming VPN client connections.

enable trigger

create trigger=1 interface=ppp0 event=up cp=ipcp script=ppp0up.scp

create trigger=2 interface=ppp0 event=up cp=ipcp script=ppp1up.scp

create trigger=3 interface=ppp0 event=up cp=ipcp script=ppp2up.scp

create trigger=4 interface=ppp0 event=up cp=ipcp script=ppp3up.scp

# See page 32 for the script each trigger runs.
```

branch office 1

Branch office 1 AR440S configuration—the PPPoA site with VPN client access and a fixed IP address

```
# SYSTEM configuration

set system name=Branch1

# USER configuration

set user securedelay=600

# Add your approved roaming VPN client usernames.

add user=roaming1 pass=roaming1 lo=no telnet=no

add user=roaming2 pass=roaming2 lo=no telnet=no

add user=roaming3 pass=roaming3 lo=no telnet=no

add user=roaming4 pass=roaming4 lo=no telnet=no

# Define a security officer.

add user=secoff pass=<your secoff password> priv=securityofficer
  lo=yes telnet=yes

# Change the manager privilege user's password.

set user=manager password=<your-password>

# RADIUS configuration

# If desired, add a RADIUS authentication server for authenticating
# users.

add radius server=<radius-server-address> secret=<secret-key>

# ATM configuration

create atm=0 over=adsl0

add atm=0 channel=1

# ADSL configuration

enable adsl=0

# PPP template configuration

# Create a template to use for incoming roaming Windows VPN client
# connections. This defines authentication and associates the IP pool
# of addresses that are allocated to clients.

create ppp template=1

set ppp template=1 bap=off ippool=roaming authentication=chap echo=10
  lqr=off

# L2TP configuration

# Configure an L2TP server to accept incoming roaming Windows VPN
# client connections

enable l2tp

enable l2tp server=both

add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1

# PPP configuration for PPPoA

# Create the PPP interface that connects the router to the internet.
# This interface needs a permanent IP address because branch office
# allows incoming roaming VPN client connections. The clients can
# only target a known, unchanging address.

create ppp=0 over=atm0.1 echo=10 lqr=off bap=off idle=off

set ppp=0 username="branch office 1" password=branch1 iprequest=off

# Note that this interface needs a permanent IP address because the
# branch office allows incoming roaming VPN client connections. The
# clients can only target a known, unchanging address.

# IP configuration

enable ip

add ip int=vlan1 ip=192.168.141.254

# Statically define the PPP interface address.

add ip int=ppp0 ip=222.222.222.1

add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0

# Create an IP pool to allocate unique internal payload addresses to
# incoming VPN clients.

create ip pool=roaming ip=192.168.143.1-192.168.143.50

# DHCP configuration

# If desired, use the router as a DHCP server.

create dhcp poli=branch1 lease=7200

add dhcp poli=branch1 rou=192.168.141.254

add dhcp poli=branch1 subn=255.255.255.0

create dhcp range=branch1_hosts poli=branch1 ip=192.168.141.16 num=32

ena dhcp

# SSH configuration

# You should not telnet to a secure gateway, so set up Secure Shell
# for remote management. This requires encryption keys - see
# "Before you start" on page 7.

# Enable the SSH server.

enable ssh server serverkey=3 hostkey=2

# Enable the user who connects via SSH to log in as secoff, by adding
# the secoff user as an SSH user. If desired, also restrict access so
# that it is only permitted from particular addresses.

add ssh user=secoff password=<secoff-password>
  ipaddress=<trusted-remote-ip-address>
  mask=<desired-subnet-mask-of-trusted-hosts>

disable telnet server

# As the commands above show, we strongly recommend SSH instead of
# telnet. However, if you choose to use telnet, create RSO users
# (remote security officers) and define the IP addresses that these
# users may connect from.

# add user rso ip=<ipadd>[-<ipadd>]

# enable user rso

# enable telnet server
```

branch office 1

```
# Log configuration

# If desired, forward router log entries to a UNIX-style syslog
# server.

create log output=2 destination=syslog
  server=<your-local-syslog-server-address> syslogformat=extended

add log out=2 filter=1 sev=>3

# IPSEC configuration

# Create an SA specification for the site-to-site VPN. This SA
# specification uses tunnel mode by default.

create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha

# Create a group of SA specifications for the roaming VPN clients.
# These SA specifications use IPsec transport mode.

create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=sha
  mod=transport

create ipsec sas=3 key=isakmp prot=esp enc=3desouter hasha=md5
  mod=transport

create ipsec sas=4 key=isakmp prot=esp enc=des hasha=sha
  mod=transport

create ipsec sas=5 key=isakmp prot=esp enc=des hasha=md5
  mod=transport

create ipsec bund=1 key=isakmp string="1"

create ipsec bund=2 key=isakmp string="2 or 3 or 4 or 5"

# Create IPsec policies to bypass IPsec for ISAKMP messages and the
# "port floated" key exchange that NAT-T uses.

create ipsec pol=isakmp int=ppp0 ac=permit

set ipsec pol=isakmp lp=500 rp=500

create ipsec pol=isakmp_float int=ppp0 ac=permit

set ipsec pol=isakmp_float lp=4500

# Create an IPsec policy for branch 1 to headquarters VPN traffic.

create ipsec pol=hq int=ppp0 ac=ipsec key=isakmp bund=1
  peer=200.200.200.1 isa=hq

set ipsec pol=hq lad=192.168.141.0 lma=255.255.255.0 rad=192.168.0.0
  rma=255.255.0.0

# Create another IPsec policy for roaming VPN clients. This policy
# uses the L2TP port to identify traffic.

create ipsec pol=roaming int=ppp0 ac=ipsec key=isakmp bund=2 peer=any
  isa=roaming

set ipsec pol=roaming lp=1701 tra=UDP

# Create another IPsec policy to allow for direct Internet access
# such as web browsing.

create ipsec pol=internet int=ppp0 ac=permit

enable ipsec
```

```
#  ISAKMP Configuration

create isakmp pol=hq pe=200.200.200.1 key=1 sendd=true heart=both

set isa pol=hq localid=branch1 encalg=3des2key

create isakmp pol=roaming pe=any key=1

set isa pol=roaming sendd=true sendi=true natt=true localid=branch1

enable isakmp

#  FIREWALL configuration

enable firewall

create firewall policy=branch1

enable firewall policy=branch1 icmp_f=all

#  Define a firewall dynamic definition to work with dynamic
#  interfaces. This provides for the dynamic PPP/L2TP interfaces that
#  incoming Windows VPN connections use.

create firewall policy=branch1 dy=roaming

add firewall policy=branch1 dy=roaming user=any

#  Specify the private and public interfaces. The roaming interface is
#  private - you can trust it because it comes from an authenticated
#  Windows VPN connection.

add firewall policy=branch1 int=vlan1 type=private

add firewall policy=branch1 int=dyn-roaming type=private

add firewall policy=branch1 int=ppp0 type=public

#  Create a NAT definition for traffic from the branch office 1 LAN to
#  use when accessing the Internet.

add firewall poli=branch1poli=branch1 nat=enhanced int=vlan1
   gblin=ppp0

#  Create another NAT definition for roaming VPN clients to use when
#  accessing the Internet via the branch office 1 router.

add firewall poli=branch1 nat=enhanced int=dyn-roaming gblin=ppp0

#  Create a rule to allow incoming ISAKMP negotiation to pass through
#  the firewall.

add firewall poli=branch1 ru=1 ac=allo int=ppp0 prot=udp po=500
   ip=222.222.222.1 gblip=222.222.222.1 gblp=500

#  Create a rule to support NAT-T. If there is a NAT gateway in the
#  VPN path, NAT-T "port floats" IKE to port 4500, and also
#  encapsulates IPsec inside the same port.

add firewall poli=branch1 ru=2 ac=allo int=ppp0 prot=udp po=4500
   ip=222.222.222.1 gblip=222.222.222.1 gblp=4500

#  Create a rule for the roaming VPN clients. Windows uses L2TP (port
#  1701) inside IPsec. This rule allows traffic that comes from IPsec
#  and uses port 1701.

add firewall poli=branch1 ru=3 ac=allo int=ppp0 prot=udp po=1701
   ip=222.222.222.1 gblip=222.222.222.1 gblp=1701 enc=ips
```

branch office 1

```
# Create a pair of rules to allow office-to-office payload traffic to
# pass through the firewall without applying NAT.
# The rule for the public interface uses encapsulation=ipsec to
# identify incoming VPN traffic.

add firewall poli=branch1 ru=4 ac=non int=ppp0 prot=all enc=ips

# The rule for the private interface uses both source and destination
# addresses to identify outgoing VPN traffic.

add firewall poli=branch1 ru=5 ac=non int=vlan1 prot=all
  ip=192.168.141.1-192.168.141.254

set firewall poli=branch1 ru=5 rem=192.168.140.0-192.168.144.254

# If you configured SSH, create a rule for SSH traffic.

add firewall policy=branch1 ru=6 ac=allo int=ppp0 prot=tcp po=22
  ip=222.222.222.1 gblip=222.222.222.1 gblp=22

# If you use telnet instead (not recommended), create a rule for it.
# add firewall policy=branch1 ru=7 ac=allo int=ppp0 prot=tcp po=23
# ip=222.222.222.1 gblip=222.222.222.1 gblp=23

# INT configuration - if prioritising VoIP

set int=ppp0 mtu=256

set int=ppp0 frag=yes

# CLASSIFIER configuration - if prioritising VoIP

# Create a classifier to identify voice traffic (DSCP value 48 in
# this example).

create class=48 ipds=48

# Software QoS configuration - if prioritising VoIP

ena sqos

# Create a traffic class. This traffic class tags the classified
# traffic as high priority on the interface queue. Also,make the
# queue small - this is optimal for VoIP traffic.

cre sqos tr=1 prio=15 maxq=10

# Create a policy with a virtual bandwidth and assign the traffic
# class to this policy.

cre sqos poli=1 virt=120kbps

add sqos poli=1 tr=1

add sqos tr=1 class=48

set sqos interface=ipsec-hq tunnelpolicy=1

# TRIGGER configuration - if prioritising VoIP

# Create triggers to apply SQoS to the dynamic PPP interfaces of up
# to four simultaneous roaming VPN client connections. See page 34
# for the script each trigger runs.

enable trigger

create trigger=1 interface=ppp0 event=up cp=ipcp script=ppp0up.scp

create trigger=2 interface=ppp0 event=up cp=ipcp script=ppp1up.scp

create trigger=3 interface=ppp0 event=up cp=ipcp script=ppp2up.scp

create trigger=4 interface=ppp0 event=up cp=ipcp script=ppp3up.scp
```

Branch office 2 AR440S configuration—the PPPoEoA site with a dynamically assigned IP address

```
# SYSTEM configuration

set system name=Branch2

# USER configuration

set user securedelay=600

# Define a security officer.

add user=secoff pass=<your secoff password> priv=securityofficer
  lo=yes telnet=yes

# Change the manager privilege user's password.

set user=manager password=<your-password>

# RADIUS configuration

# If desired, add a RADIUS authentication server for authenticating
# users.

add radius server=<radius-server-address> secret=<secret-key>

# ATM configuration

create atm=0 over=adsl0

add atm=0 channel=1

# ETH configuration

# Create a virtual ethernet interface over ATM.

create eth=0 over=atm0.1

# ADSL configuration

enable adsl=0

# PPP configuration for PPPoE

# Create the PPP interface that the router uses to connect to the
# ISP. Use iprequest=on so that the interface obtains its address
# dynamically from the ISP.

create ppp=0 over=eth0-any echo=10 lqr=off bap=off idle=off

set ppp=0 iprequest=on username="branch office 2" password=branch2
  pass

# IP configuration

enable ip

add ip int=vlan1 ip=192.168.142.254

# Configure a temporary null address, because the interface gets its
# address through remote assignment.

enable ip remote

add ip int=ppp0 ip=0.0.0.0

add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
```

branch office 2

```
# DHCP configuration

# If desired, use the router as a DHCP server.

create dhcp poli=branch2 lease=7200

add dhcp poli=branch2 rou=192.168.142.254

add dhcp poli=branch2 subn=255.255.255.0

create dhcp range=branch2_hosts poli=branch2 ip=192.168.142.16 num=32

ena dhcp

# SSH configuration

# You should not telnet to a secure gateway, so set up Secure Shell
# for remote management. This requires encryption keys - see
# "Before you start" on page 7.

# Enable the SSH server.

enable ssh server serverkey=2 hostkey=3

# Enable the user who connects via SSH to log in as secoff, by adding
# the secoff user as an SSH user. If desired, also restrict access so
# that it is only permitted from particular addresses.

add ssh user=secoff password=<secoff-password>
  ipaddress=<trusted-remote-ip-address>
  mask=<desired-subnet-mask-of-trusted-hosts>

disable telnet server

# As the commands above show, we strongly recommend SSH instead of
# telnet. However, if you choose to use telnet, create RSO users
# (remote security officers) and define the IP addresses that these
# users may connect from.

# add user rso ip=<ipadd>[-<ipadd>]

# enable user rso

# enable telnet server

# Log configuration

# If desired, forward router log entries to a UNIX-style syslog
# server.

create log output=2 destination=syslog
  server=<your-local-syslog-server-address> syslogformat=extended

add log out=2 filter=1 sev=>3

# IPSEC configuration

# Create an SA specification for the site-to-site VPN. This SA
# specification uses tunnel mode by default.

create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha

create ipsec bund=1 key=isakmp string="1"

# Create an IPsec policy to bypass IPsec for ISAKMP messages.

create ipsec pol=isakmp int=ppp0 ac=permit

set ipsec pol=isakmp lp=500 rp=500
```

```
# Create an IPsec policy for branch 2 to headquarters VPN traffic.

create ipsec pol=hq int=ppp0 ac=ipsec key=isakmp bund=1
  peer=200.200.200.1 isa=hq

set ipsec pol=hq lad=192.168.142.0 lma=255.255.255.0 rad=192.168.0.0
  rma=255.255.0.0

# Create another IPsec policy to allow for direct Internet access
# such as web browsing.

create ipsec pol=internet int=ppp0 ac=permit

enable ipsec

# ISAKMP Configuration

create isakmp pol=hq pe=200.200.200.1 key=1 sendd=true heart=both

set isakmp pol=hq localid=branch2 encalg=3des2key

enable isakmp

# FIREWALL configuration

enable firewall

create firewall policy=branch2

enable firewall policy=branch2 icmp_f=all

# Specify the private and public interfaces.

add firewall policy=branch2 int=vlan1 type=private

add firewall policy=branch2 int=ppp0 type=public

# Create a NAT definition for traffic from the branch office 2 LAN to
# use when accessing the Internet.

add firewall poli=branch2 nat=enhanced int=vlan1 gblin=ppp0

# Create a rule to allow incoming ISAKMP negotiation to pass through
# the firewall. This rule specifies 0.0.0.0 as the global IP address
# because the PPP address of branch office 2 is dynamically assigned.
# The rule uses the LAN address to identify matching traffic.

add firewall poli=branch2 ru=1 ac=allo int=ppp0 prot=udp po=500
  ip=192.168.142.254 gblip=0.0.0.0 gblp=500

# Create a pair of rules to allow office-to-office payload traffic to
# pass through the firewall without applying NAT.
# The rule for the public interface uses encapsulation=ipsec to
# identify incoming VPN traffic.

add firewall poli=branch2 ru=4 ac=non int=ppp0 prot=all enc=ips

# The rule for the private interface uses both source and destination
# addresses to identify outgoing VPN traffic.

add firewall poli=branch2 ru=5 ac=non int=vlan1 prot=all
  ip=192.168.142.1-192.168.142.254

set firewall poli=branch2 ru=5 rem=192.168.140.0-192.168.144.254

# If you configured SSH, create a rule for SSH traffic.

add firewall policy=branch2 ru=6 ac=allo int=ppp0 prot=tcp po=22
  ip=192.168.142.254 gblip=0.0.0.0 gblp=22
```

```
# If you use telnet instead (not recommended), create a rule for it.
# add firewall policy=branch2 ru=7 ac=allo int=ppp0 prot=tcp po=23
# ip=192.168.142.254 gblip=0.0.0.0 gblp=23

# INT configuration - if prioritising VoIP

set int=ppp0 mtu=256

set int=ppp0 frag=yes

# CLASSIFIER configuration - if prioritising VoIP

# Create a classifier to identify voice traffic (DSCP value 48 in
# this example).

create class=48 ipds=48

# Software QoS configuration - if prioritising VoIP

ena sqos

# Create a traffic class. This traffic class tags the classified
# traffic as high priority on the interface queue. Also,make the
# queue small - this is optimal for VoIP traffic.

cre sqos tr=1 prio=15 maxq=10

# Create a policy with a virtual bandwidth and assign the traffic
# class to this policy.

cre sqos poli=1 virt=120kbps

add sqos poli=1 tr=1

add sqos tr=1 class=48

set sqos interface=ipsec-hq tunnelpolicy=1
```

Extra configuration scripts for lab testing the VPN solution

This section provides additional configuration that you may need if you want to lab test the VPN solution. It has scripts for:

- setting up a PPPoE access concentrator for branch office 2 to connect to. In a test network, this access concentrator plays the role of the PPPoA or PPPoEoA service from your ISP or Telco
- setting up a NAT gateway so you can verify your VPN clients passing through NAT-T. In a test network, this NAT gateway router plays the role of the hotel's NAT gateway.

ISP's PPPoE access concentrator configuration

This configuration is provided only to allow you to bench test this VPN solution. In the live installation, your ISP or Telco provides your PPPoEoA or PPPoA service.

```
# SYSTEM configuration

set system name=ISP

# USER configuration

# Create user definitions for authenticating incoming PPPoE
# connections

add user="branch office 1" pass="branch 1" lo=no ip=222.222.222.1
  mask=255.255.255.255 telnet=no

# For the branch office 2 user, use 222.222.222.3. This represents
# the dynamically assigned address that the ISP assigns in a live
# network.

add user="branch office 2" pass="branch 2" lo=no ip=222.222.222.3
  mask=255.255.255.255 telnet=no

# PPP templates configuration

create ppp template=1

set ppp template=1 authentication=chap echo=10 lqr=off bap=off
  idle=off

# PPP configuration

# Enable the PPPoE access concentrator service

add ppp acservice=training template=1 maxsessions=20

ena ppp accessconcentrator

# IP configuration

enable ip

add ip int=eth0 ip=222.222.222.254

add ip int=eth1 ip=200.200.200.254

add ip int=eth2 ip=211.211.211.254
```

Hotel's NAT gateway firewall configuration

```
# SYSTEM configuration
set system name=Hotel
# IP configuration
enable ip
add ip int=eth0 ip=211.211.211.1
add ip int=eth1 ip=192.168.200.254
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=211.211.211.254
# FIREWALL configuration
enable firewall
create firewall policy=hotel
enable firewall policy=hotel icmp_f=all
add firewall policy=hotel int=eth1 type=private
add firewall policy=hotel int=eth0 type=public
add firewall poli=hotel nat=enhanced int=eth1 gblin=eth0
```

USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

Connecting The IP World

Allied Telesis™